Partial Translation of Japanese Unexamined Patent Publication (Kokai) No. 06-274419

Date of publication: September 30, 1994
Application number: 05-86930
Date of filing: March 23, 1993

Title of the Invention: INFORMATION RECORDING MEDIUM AND DATA RECORDING METHOD FOR THE SAME

Applicant: Mitsubishi Kasei Corp.
Inventors: Susumu Haraki
Ryuhei Sato

1. Paragraph Numbers [0006] to [0014] in "Detailed Description of the Invention"

[0006]

After conducting intensive studies on how computer viruses can intrude into a computer system, the present inventors have discovered that providing a read-only storage area in a portion of a rewritable information recording medium and including a virus check program as device driver software into the read-only storage area is particularly effective not only in protecting the data stored in the rewritable data recording area from computer viruses but also in preventing computer viruses from being spread to other computer systems, and have completed the present invention based on this discovery.

[0007]

That is, the information recording medium of the present invention, which achieves the above object, has a rewritable data recording area and a read-only storage area, wherein at least a portion of a virus check program which, upon occurrence of a write instruction to the data recording area, issues an instruction to a computer to

check for the presence of a computer virus is recorded as device driver software in the read-only storage area.

[0008]

Further, the data recording method for a computer information recording medium according to the present invention is characterized in that the information recording medium has a rewritable data recording area and a read-only storage area, and in that at least a portion of a virus check program is recorded as device driver software in the read-only storage area and, upon occurrence of a write instruction to the data recording area, the virus check program checks for the presence of a computer virus, thereby preventing the data recording area from being infected with a computer virus.

[0009]

The phrase "to check for the presence of a computer virus" used in this specification means either checking if a computer virus is included within a particular program or data, or checking if a particular instruction issued to the computer system is an instruction issued by a computer virus, or both.

[0010]

Further, the "device driver software" refers to a program which, for example, like a front-end processor (FEP), a clock program, a calculator program, or the like, is loaded into the computer main memory when the computer is started up, and remains in the memory thereby adding functionality not provided by the computer controlling operating system, to the computer system.

[0011]

If the virus check program that issued the instruction

to check for the presence of a computer virus has detected that a computer virus is included in the program or data to be written to the data recording area, a notification to that effect is, for example, displayed on the screen to notify the user and, at the same time, the writing of that data is inhibited. Further, if a particular instruction is judged to be an instruction issued by a computer virus, a notification to that effect is, for example, sent to the user and, at the same time, that instruction is removed. With these instructions, computer virus intrusion and its effects can be prevented.

[0012]

The whole virus check program may be recorded as a single piece of device driver software, or alternatively, it may be recorded by being divided into two sections, for example, a device driver section which detects the occurrence of an external data write and an application section which is activated by the device driver section when the occurrence of an external data write is detected. One or the other, whichever is suitable, can be chosen by considering the main memory capacity of the computer system, the speed required for data recording, etc.

[0013]

Since the whole virus check program is recorded in the read-only storage area, the program can be prevented from being accidentally erased by the user or from being destroyed by a computer virus. Accordingly, as long as the information recording medium is started up by the computer system, the program constantly checks external data to be written to the data recording area and its write instruction, so that computer virus intrusion and its

effects can be prevented.

[0014]

[Mode of Operation] Since at least a portion of the virus check program that issues an instruction to check for the presence of a computer virus is recorded as device driver software in the read-only storage area, the virus check program works during the operation of the computer system to block computer viruses from entering the rewritable data recording area or affecting the data recorded therein. In this way, the information recording medium not only can be protected from computer viruses but can also be prevented from spreading computer viruses, regardless of the user's awareness of computer viruses.

2. Paragraph Number [0023] in "Detailed Description of the Invention"

[0023]

For the above purpose, the first program section contains pattern data about the patterns of typical or various known viruses, and compares the pattern contained in the external data against the pattern data. The information recording medium can be configured so that any new computer virus known after the manufacture of the recording medium can be added as additional pattern data to the MO area of the recording medium.

3. Paragraph Number [0031] in "Detailed Description of the Invention"

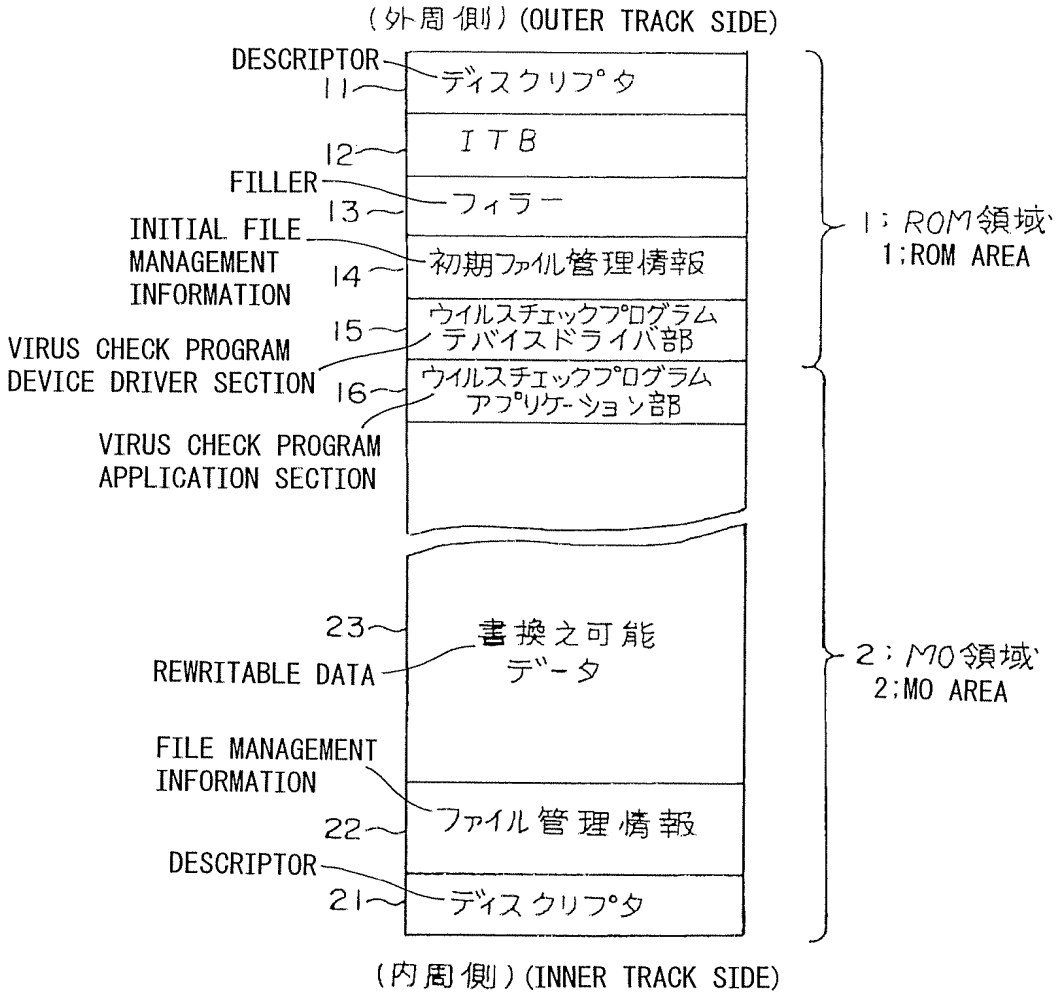
[0031]

According to the virus check program of the above embodiment, since the possibility is eliminated that external data containing a virus may enter the MO area or that the system data, etc., in the MO area may be altered

directly by an external instruction before the user is aware of it, programs and data recorded in the MO area of the information recording medium can be prevented from being destroyed by computer viruses. Since the virus check program performs the virus check without requiring the user to perform any extra processing, the operation can be performed without giving any burden to the user.

[Translation of the Drawing]

[FIG. 2] [図2]



(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06274419 A**

(43) Date of publication of application: **30.09.94**

(51) Int. Cl **G06F 12/14**
G06F 9/06
G11B 13/00
G11B 20/12

(21) Application number: **05086930**

(22) Date of filing: **23.03.93**

(71) Applicant: **MITSUBISHI KASEI CORP**

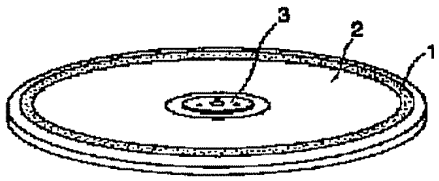
(72) Inventor: **HARAKI SUSUMU**
SATO RYUHEI

(54) INFORMATION RECORDING MEDIUM AND RECORDING METHOD DATA THEREOF

(57) Abstract:

PURPOSE: To protect data recorded in the information recording medium from being broken down by a computer virus.

CONSTITUTION: The information recording medium such as a magneto-optical disk, etc., is provided with a read-only storage area in which a virus check program is recorded as a device driver software. When a command for writing external data is generated in a rewritable data recording area 2 of the information recording medium, whether a computer virus exists in its external data or write command or not is checked by this virus check program. The virus check program is recorded in the read-only storage area 1 by a manufacturer of the information recording medium, therefore, there is no possibility of infection of a virus, and also, when a computer system is operated, it rises automatically, therefore, a burden for a processing is not imposed on a user. A breakdown by the computer virus of data recorded in the information recording medium, and expansion of the computer virus through the medium of this information recording medium are both prevented.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平6－274419

(43)公開日　平成６年(1994)９月30日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３１０　Ａ	9293－5B		
9/06	４５０　Ｚ	9367－5B		
Ｇ１１Ｂ　13/00		9075－5D		
20/12		9295－5D		

審査請求　未請求　請求項の数４　ＦＤ　（全　７　頁）

(21)出願番号　特願平5－86930

(22)出願日　平成５年(1993)３月23日

(71)出願人　000005968
三菱化成株式会社
東京都千代田区丸の内二丁目５番２号

(72)発明者　原木　晋
神奈川県横浜市緑区鴨志田町1000番地　三菱化成株式会社総合研究所内

(72)発明者　佐藤　龍平
東京都千代田区丸の内二丁目５番２号　三菱化成株式会社内

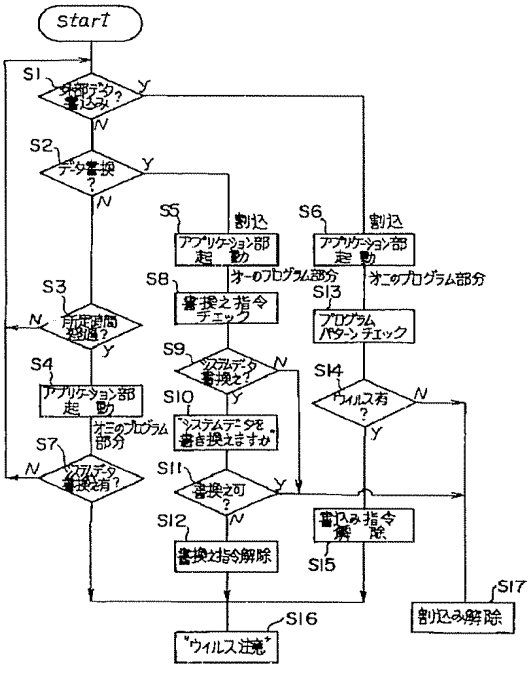
(74)代理人　弁理士　稲垣　清

(54)【発明の名称】　情報記録媒体及びそのデータの記録方法

(57)【要約】

【目的】　情報記録媒体に記録されたデータをコンピュータウイルスによる破壊から守る。

【構成】　光磁気ディスク等の情報記録媒体に、ウイルスチェックプログラムがデバイスドライバ・ソフトウエアとして記録された読出し専用記憶領域を設ける。情報記録媒体の書換え可能なデータ記録領域に外部データを書き込む指令が発生したときに、このウイルスチェックプログラムにより、その外部データ又は書込み指令にコンピュータウイルスが存在するか否かをチェックする。ウイルスチェックプログラムは、読出し専用記憶領域に情報記録媒体の製造者によって記録されるので、ウイルスによる感染のおそれがなく、また、コンピュータシステムの作動時には、自動的に立上がるので、ユーザに処理上の負担をかけることもない。情報記録媒体に記録されたデータのコンピュータウイルスによる破壊と、この情報記録媒体を媒介としてのコンピュータウイルスの拡大との双方を防止する。



1

【特許請求の範囲】

【請求項１】　書換え可能なデータ記録領域及び読出し専用記憶領域を備え、前記データ記録領域への書込み指令が発生したときにコンピュータウイルスの存在の有無をチェックする指令をコンピュータに与えるウイルスチェックプログラムの少なくとも一部を、デバイスドライバ・ソフトウエアとして前記読出し専用記憶領域に記録したことを特徴とする情報記録媒体。

【請求項２】　前記ウイルスチェックプログラムは、前記書込み指令の発生を監視するデバイスドライバ部と、前記書込み指令が発生したときに該デバイスドライバ部により起動されるアプリケーション部とから構成されることを特徴とする請求項１に記載の情報記録媒体。

【請求項３】　前記書換え可能なデータ領域が光磁気領域であり、前記読出し専用記憶領域のデータが光学的に読取が可能なデータとして記録されることを特徴とする請求項１又は２に記載の情報記録媒体。

【請求項４】　情報記録媒体に書換え可能なデータ記録領域及び読出し専用記憶領域を設け、
前記読出し専用記憶領域にウイルスチェックプログラムの少なくとも一部をデバイスドライバ・ソフトウエアとして記録し、
前記データ記録領域への書込み指令が発生したときに、コンピュータウイルスの存在の有無を前記ウイルスチェックプログラムによりチェックすることにより、前記データ記録領域へのコンピュータウイルスの侵入を防止する、コンピュータのための情報記録媒体のデータの記録方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、情報記録媒体及びそのデータの記録方法に関し、更に詳しくは、書換え可能なデータ記録領域に加えて読出し専用記憶領域を設けた、コンピュータのための情報記録媒体及びそのデータの記録方法に関する。

【０００２】

【従来の技術】近年、メディア交換が可能な情報記録装置或いは通信ネットワークを介して、コンピュータウイルスが伝達され、コンピュータシステム内に蓄えられた重要なプログラムやデータが破壊される事例がしばしば報告されている。コンピュータウイルスは、一般に、プログラムやデータと共に情報記録媒体又は通信ネットワークから侵入する。かかるコンピュータウイルスの侵入を防止することについては、例えば、コンピュータシステムにウイルスチェックの機能を持たせる例があり、また、プログラムやデータの安易なコピーをしない等、コンピュータシステムの運用上で種々の提案がなされている。

【０００３】しかし、コンピュータシステム自体にウイルスチェック機能を持たせることは、必ずしも全てのコンピュータシステムに可能とはいえない。ウイルスチェックの機能を有しないコンピュータシステムの場合、コンピュータウイルスについて知識が充分でないユーザは、コンピュータウイルスを無防備に受け入れてしまい、自身のプログラム及びデータの破壊のみならず、受け入れたコンピュータウイルスを他に伝達しがちである。コンピュータウイルスは、かかるユーザのコンピュータシステムを媒介として急速に拡大し、多数のコンピュータシステムのデータを破壊する等、しばしば大きな社会的影響を与える。

2

【０００４】

【発明が解決しようとする課題】例えば光磁気ディスク等、メディア交換ができ、大量のデータが記録できる書換え可能な情報記録媒体にあっては、そのメディア交換が可能である特長のためウイルスによる感染の機会が多く、且つ、その大量のデータを蓄積できる性質上、コンピュータウイルスによって特に重大な被害を被ることが考えられる。しかし、従来は、前記の如くコンピュータシステム自体の機能及びユーザの意識等に任されていたため、コンピュータウイルスによる情報記録媒体の大量のデータ破壊、並びに情報記録媒体による他のコンピュータシステムへのコンピュータウイルスの媒介について、効果的に防止することができなかった。

【０００５】本発明は、上記に鑑み、蓄積されたデータをコンピュータウイルスから守り、且つコンピュータウイルスを他のコンピュータシステムに媒介しないことを可能とする情報記録媒体及びそのデータの記録方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明者らは、コンピュータシステムへのコンピュータウイルスの侵入の態様について鋭意研究を重ね、書換え可能な情報記録媒体の一部に読出し専用記憶領域を設け、この読出し専用記憶領域にウイルスチェックのためのプログラムをデバイスドライバ・ソフトウエアとして組込むことが、書換え可能なデータ記録領域に格納されたデータをコンピュータウイルスから守り、且つ、他のコンピュータシステムにコンピュータウイルスを媒介しないことについて特に有効であることに想到し、本発明を完成するに至った。

【０００７】即ち、前記目的を達成する本発明の情報記録媒体は、書換え可能なデータ記録領域及び読出し専用記憶領域を備え、前記データ記録領域への書込み指令が発生したときにコンピュータウイルスの存在の有無をチェックする指令をコンピュータに与えるウイルスチェックプログラムの少なくとも一部を、デバイスドライバ・ソフトウエアとして前記読出し専用記憶領域に記録したことを特徴とするものである。

【０００８】また、本発明のコンピュータのための情報記録媒体のデータの記録方法は、情報記録媒体に書換え可能なデータ記録領域及び読出し専用記憶領域を設け、

前記読出し専用記憶領域にウイルスチェックプログラムの少なくとも一部をデバイスドライバ・ソフトウエアとして記録し、前記データ記録領域への書込み指令が発生したときに、コンピュータウイルスの存在の有無を前記ウイルスチェックプログラムによりチェックすることにより、前記データ記録領域へのコンピュータウイルスの侵入を防止することを特徴とするものである。

【０００９】本明細書において使用する、「コンピュータウイルスの存在の有無をチェックする」とは、ある特定のプログラム又はデータの内部にコンピュータウイルスが含まれるか否かを調べること、及び、コンピュータシステムに与えられる特定の指令がコンピュータウイルスによる指令か否かをチェックすることの一方又は双方を意味するものである。

【００１０】また、「デバイスドライバ・ソフトウエア」とは、例えば、フロントエンドプロセッサ（ＦＥＰ）、時計用プログラム、電卓用プログラム等と同様なプログラムの一つであり、一般に、コンピュータの起動時に、コンピュータの主記憶装置内に読み込まれて常駐することで、コンピュータを制御するオペレーティングシステムが有しない機能をコンピュータシステムに付加するプログラムをいう。

【００１１】コンピュータウイルスの存在の有無をチェックする指令を与えるウイルスチェックプログラムにより、データ記録領域に書込むべきプログラム又はデータにコンピュータウイルスが含まれていると検出された場合には、例えば、その旨を画面上に表示してユーザに知らせると共にそのデータの書込みを禁止する。また、特定の指令がコンピュータウイルスによる指令であると判定される場合には、例えば、ユーザにその旨を知らせると共にその指令を解除する。これらの指令により、コンピュータウイルスの侵入乃至はその影響を防止できる。

【００１２】ウイルスチェックプログラムは、全体を１つのデバイスドライバ・ソフトウエアとすることができ、また、例えば外部データの書込み発生を検出するデバイスドライバ部と、外部データの書込み発生が検出された際に、このデバイスドライバ部によって起動されるアプリケーション部との２つの部分に分離して記録することもできる。いずれを採用するかは、コンピュータシステムの主記憶装置の容量、データ記録時に要求されるスピード等を勘案して適宜選択できる。

【００１３】ウイルスチェックプログラム全体を読出し専用記憶領域に記録すれば、このプログラムは、ユーザにより誤って消去されることがなく、また、コンピュータウイルスによっても消去されないので、コンピュータシステムにより情報記録媒体が起動される限り、常にデータ記録領域への書込みをが行われる外部データ又はその書込み指令をチェックして、コンピュータウイルスの侵入又はその影響を阻止することが出来る。

【００１４】

【作用】コンピュータウイルスの存在の有無をチェックする指令を与えるウイルスチェックプログラムの少なくとも一部を、デバイスドライバ・ソフトウエアとして読出し専用記憶領域に記録する構成により、コンピュータシステムの作動中は、ウイルスチェックプログラムの機能により、書換え可能なデータ記録領域にコンピュータウイルスが侵入し或いはそのデータに影響を与えることが防止できるので、ユーザのコンピュータウイルスに対する意識の如何を問わず、コンピュータウイルスに感染せず、且つコンピュータウイルスを媒介しない情報記録媒体とすることが出来る。

【００１５】

【実施例】図面を参照して本発明を説明する。図１は本発明の一実施例の情報記録媒体を成す光磁気ディスクを示す斜視図である。同図において、この光磁気ディスクは、その書換え可能な光磁気記録領域（以下ＭＯ領域と呼ぶ）に加えて、光学的に読出しが可能な読出し専用記憶領域（以下ＲＯＭ領域と呼ぶ）を一部に設けた形式のＰ－ＲＯＭ（バーシャルＲＯＭ）型光磁気ディスクとして構成されている。

【００１６】Ｐ－ＲＯＭ型光磁気ディスクは、例えば厚みが数ｍｍで直径が１００ｍｍ程度のディスク状をなしており、ディスクの外周側にＲＯＭ領域１、内周側に書換え可能なＭＯ領域２を有する。ＭＯ領域２の更に内周側には、ディスク駆動装置からの回転駆動力を受けるハブ３が配置されている。

【００１７】ＲＯＭ領域１内の情報は、エンボス加工によるディスク表面の凹凸ピットデータとして、ディスクの製作者側で画一的に形成される。このＲＯＭ領域１内の情報は、光磁気ディスク駆動装置においてレーザ光の明暗により読み取られる。また、ＭＯ領域２内のデータは、コンピュータシステムの制御を受けたディスク駆動装置において、レーザ光及び磁気ヘッドを利用した光学的且つ磁気的方法によりユーザ側で記録・再生される。ディスクの全体は、図示しない框体を成すジャケット内に収容されている。

【００１８】図２は、図１のＰ－ＲＯＭ型光磁気ディスクについて、その使用開始後における各領域のデータ配置を模式的に例示する。ＲＯＭ領域１には、外周側から順に、ディスク管理のために使用されるディスクリブタが記録されたエリア１１、ＲＯＭ領域の情報をＭＯ領域にコピーするための手順及び位置情報等を与える情報が記録されたエリアＩＴＢ１２、未使用エリアを成すフィラー１３、初期ファイル管理情報が記録されたエリア１４、ウイルスチェックプログラムの一部を構成するデバイスドライバ部が記録されたエリア１５、及び、ウイルスチェックプログラムの他の一部を構成するアプリケーション部が記録されたエリア１６が順次配置されている。なお、これらに加えて他の情報を記録することもできる。

5

【００１９】ＭＯ領域２は、ディスクの大部分を占める領域であり、例えば数百バイトの記録容量を有する１セクタを単位とする領域が円周方向及び半径方向に配列された領域集合として構成され、全体として、例えば約１００～６００メガバイト程度の記録容量を有する。ＭＯ領域２内には、その最も内周側に、光磁気ディスクのフォーマットに際してＲＯＭ領域１からコピーされたディスクリプタ及びファイル管理情報が記録されるエリア２１、２２が配置される。

【００２０】ディスクリプタ及びファイル管理情報が記録されたエリア２１及び２２の外周側には、書換え可能なデータエリア２３が配置される。この光磁気ディスクをシステムドライバとして使用する場合には、一般に、この書換え可能なデータエリアにコンピュータのオペレーティングシステムが記録される。オペレーティングシステムは、その一部が書込み可能なデータエリア２３の特定位置に記録される。

【００２１】デバイスドライバ部は、コンピュータシステムの作動中、ＭＯ領域に外部データが書き込まれることを監視し、新たに外部データを書き込む指令が発生すると、或いは、ＭＯ領域のデータを書き換える外部指令が発生すると、その書込み又は書換えの実行に先立ってアプリケーション部を起動する。アプリケーション部は、例えば、以下のような指令をコンピュータに与えるプログラム部分を含んでいる。

【００２２】第一のプログラム部分は、書換え可能なデータ記録領域に新たに書き込まれるべき外部データ（外部プログラムを含む）のパターンをチェックする指令である。一般に、コンピュータウイルスは、割込み処理を頻繁にかける、或いは、特定位置に記録されたオペレーティングシステムを書き換える指令を有する等、特異なプログラムパターンを有している。第一のプログラム部分は、書込み指令が発生した外部データのパターンをチェックした結果、その外部データがコンピュータウイルスに特有のプログラムパターンを有している場合には、その旨をユーザに知らせ、同時に、例えばそのような疑いのあるプログラムの書込み指令を自動的に解除する。

【００２３】上記目的のために、第一のプログラム部分は、典型的な又は既知の各ウイルスの夫々のパターンをパターンデータとして保有し、このパターンデータと外部データに含まれるパターンとの照合を行う。情報記録媒体が製作された後に知られた新たなコンピュータウイルスのパターンは、追加のパターンデータとして与えられ、情報記録媒体のＭＯ領域に付加する構成が採用できる。

【００２４】第二のプログラム部分は、データの書換え指令がコンピュータウイルスによるものか否かをチェックする。種々の手法が考えられるが、この実施例では、書換指令を受けたＭＯ領域内のデータがオペレーティングシステム或いはシステムのブートストラップ等、一般

6

に書換えが行われないプログラム等を書き換えるものかどうかをチェックすることによりこれを行う。例えば、オペレーティングシステムで且つ記録されるエリアが予め定められているシステムプログラムの場合には、当該エリアを書き換える指令であるか否かをチェックすることにより、オペレーティングシステムの書換えであると容易に判定できる。

【００２５】書換え指令が、通常頻繁には書換えが行われない特定のシステムデータの書換え指令であると検出された場合には、例えば、ディスプレイ画面上に「システムデータを書き換えますか」等の表示を行い、ユーザの注意を喚起する。ユーザより、システムデータを書き換える旨の指示が与えられた場合に限り書換えを許可し、その他の場合には、書換え指令を解除し、更にコンピュータウイルスに関する情報を画面上に表示してユーザに注意を喚起する。

【００２６】第三のプログラム部分は、ウイルスによる感染の有無をチェックする指令を与える。このプログラム部分は、例えば、通常は頻繁に書換えが行われない重要なシステムデータについてバックアップファイルを作成しておき、定期的にデバイスドライバにより起動されて、システムデータとそのバックアップデータとを照合することにより、システムデータの書換えの有無をチェックする。データの書換えが検出された場合には、その旨についてユーザの注意を喚起する。

【００２７】図３に、上記実施例の情報記録媒体における、また、本発明の一実施例による情報記録媒体のデータの記録方法における、ウイルスチェックの処理ルーチンを例示した。同図において、ステップＳ１～ステップＳ６の処理は、デバイスドライバ部の指令により行われ、その他のステップＳ７～Ｓ１７の処理はアプリケーション部の指令により行われる。デバイスドライバ部は、ＭＯ領域に外部データの書込み指令があるか否か（Ｓ１）、及びＭＯ領域のデータを直接に書き換える指令があるか否か（Ｓ２）を常時監視している。また、システムデータの書換えが行われたか否かを定期的にチェックする（Ｓ３及びＳ７）。

【００２８】デバイスドライバ部は、ステップＳ１で外部データの書込み指令が発生した場合には、コンピュータシステムに割込みをかけ、同時にアプリケーション部を起動する（Ｓ６）。アプリケーション部の第一のプログラム部分により、外部データのプログラムパターンのチェックが行われる（Ｓ１３）。ウイルスの存在が検出された場合には（Ｓ１４）、外部データの書込み指令を解除し（Ｓ１５）、例えば画面上に「ウイルス注意」の表示を行い（Ｓ１６）、ユーザに注意を喚起して処理を終了する。また、ウイルスが発見されない場合には割込みを解除して、外部データの書込みを許可する（Ｓ１７）。

【００２９】ステップＳ２でＭＯ部のデータを直接に書

き換える指令が検出された場合には、同様に、アプリケーション部が起動される（Ｓ５）。アプリケーション部の第二のプログラム部分の指令により、バッファ内部の書換え指令の内容がチェックされる（Ｓ８）。書換え指令がシステムデータ又はブートストラップ等の書換えでない場合には（Ｓ９）、そのまま割込みを解除し、書換えを許可して処理を終了する（Ｓ１７）。

【００３０】ステップＳ９で、書換え指令がシステムデータ等を書き換えるものである場合には、ディスプレイ画面上に、例えば「システムデータを書き換えますか」の表示を行い（Ｓ１０）、ユーザから「書換え可」の旨の入力があった場合には（Ｓ１１）、そのまま処理を終了し、また、「書換え不可」の旨の入力があった場合には、書換え指令を解除して（Ｓ１２）、「ウイルス注意」等の表示によりユーザに注意を喚起する（Ｓ１６）。

【００３１】上記実施例におけるウイルスチェックプログラムによると、ウイルスを含んだ外部データをＭＯ領域に受け入れたり、或いは、外部からの直接の指令によりＭＯ領域のシステムデータ等がユーザの知らない間に外部データにより書き換えられたりするおそれが解消するので、情報記録媒体のＭＯ領域に記録されたプログラム及びデータをコンピュータウイルスによる破壊から守ることができる。ウイルスチェックプログラムは、ユーザによる特別な処理を要することなくウイルスチェック処理を行うので、ユーザに処理上の負担を与えることはない。

【００３２】また、上記実施例では、ウイルスチェックプログラムを、デバイスドライバ部とアプリケーション部とに分離する構成を採用したことにより、コンピュータシステムの作動中にその主記憶装置に格納されるデバイスドライバの容量を小さく抑えることができる。

【００３３】更に、上記実施例では、デバイスドライバ部及びアプリケーション部は、いずれも光磁気ディスクのＲＯＭ領域に、ディスク表面の凹凸情報として記録されており、ウイルスによる感染とは無縁である。従って、コンピュータシステムにおいて光磁気ディスクが使用される限り、その光磁気ディスクの機能によりウイルスチェックが行われる。

【００３４】上記の如く、上記実施例の情報記録媒体及＊びそのデータの記録方法によると、ユーザがコンピュータウイルスの排除を意識するか否かに拘らず、情報記録媒体の機能により情報記録媒体へのコンピュータウイルスの侵入或いはその影響の防止が可能となり、書換え可能なデータ記録領域に蓄積されたデータをコンピュータウイルスによる破壊から守ることができる。また、この情報記録媒体を通してコンピュータウイルスが媒介されることもないので、コンピュータウイルスの拡大を防止できる。

【００３５】なお、上記実施例の構成は、単に例示の目的で記述されたものであり、本発明の情報記録媒体及びそのデータの記録方法は、特に上記実施例の構成に限定されるものではなく、種々の変形修正が可能である。例えば、情報記録媒体が光磁気ディスクに限定されるものではない。

【００３６】

【発明の効果】以上説明したように、本発明によると、情報記録媒体へのコンピュータウイルスの侵入又はその影響を防止できるので、情報記録媒体に記録されたデータを破壊から守ることができ、また、この情報記録媒体からコンピュータウイルスが伝達されることもないので、コンピュータウイルスの拡大が防止できる。

【図面の簡単な説明】

【図１】本発明の一実施例の情報記録媒体を成すＰ－ＲＯＭ型光磁気ディスクの構造を示す斜視図。

【図２】図１の実施例の光磁気ディスクにおけるデータの配置を模式的に例示するブロック図。

【図３】図１及び２の実施例の情報記録媒体、並びに、本発明の一実施例の情報記録媒体のデータの記録方法における処理を例示するフロー図。

【符号の説明】

１：ＲＯＭ（読出し専用記憶）領域

１５：ウイルスチェックプログラムのデバイスドライバ部

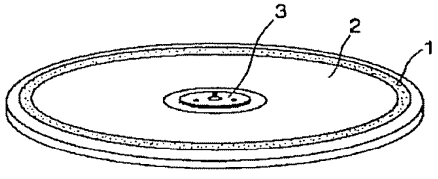
１６：ウイルスチェックプログラムのアプリケーション部

２：ＭＯ（光磁気記録）領域

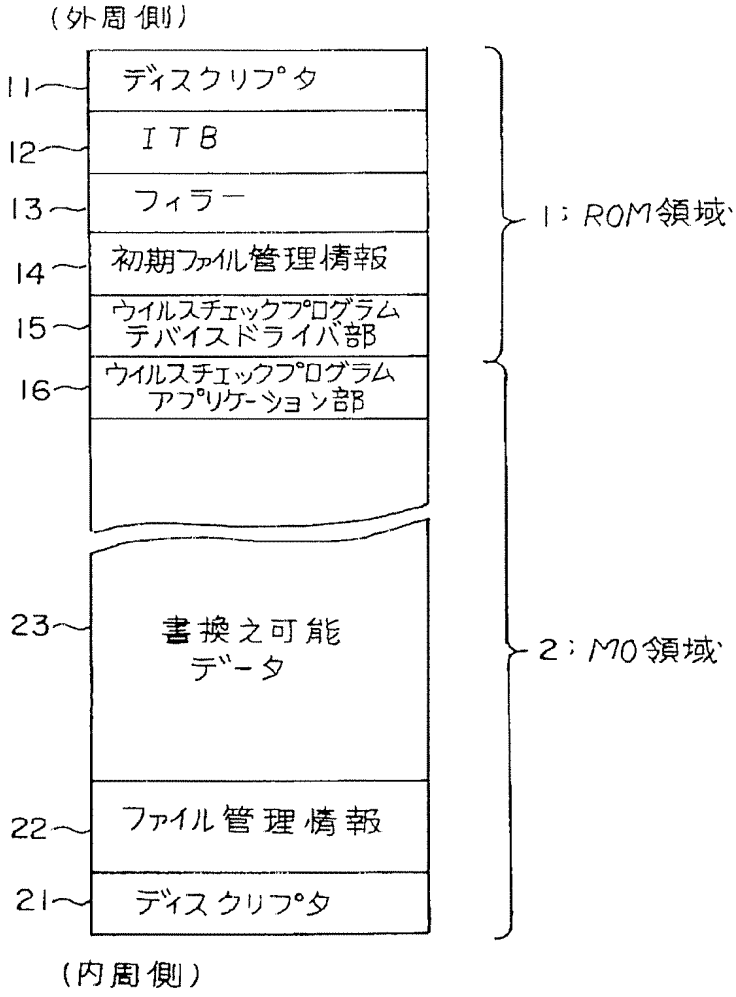
２２：ファイル管理情報エリア

２３：書換え可能なデータエリア

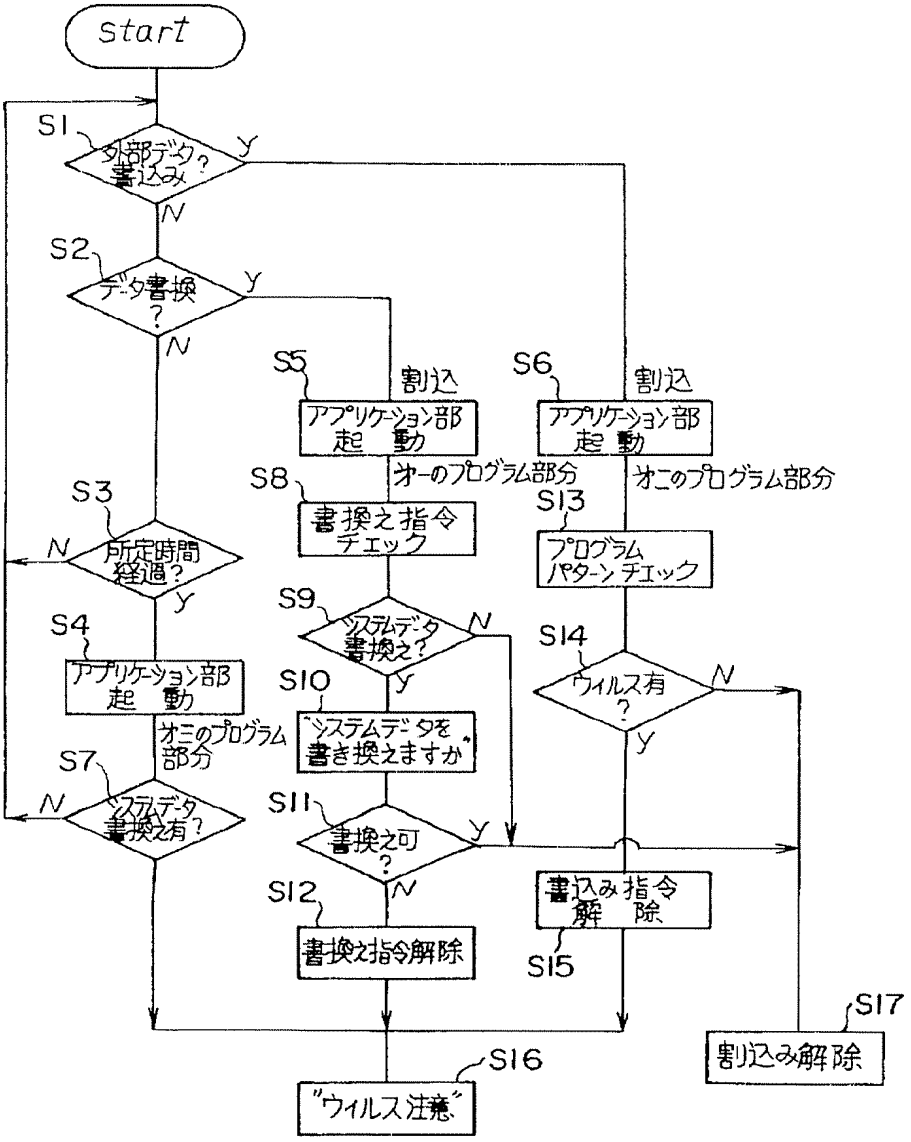
【図１】



【図２】


（外周側）
11
ディスクリプタ
12
ＩＴＢ
13
フィラー
14
初期ファイル管理情報
15
ウイルスチェックプログラム
デバイスドライバ部
16
ウイルスチェックプログラム
アプリケーション部
23
書換え可能
データ
22
ファイル管理情報
21
ディスクリプタ
1：ROM領域
2：MO領域
（内周側）

【図３】


Start
S1
外部データ書込み?
Y
N
S2
データ書換?
Y
N
S3
所定時間経過?
N
Y
S4
アプリケーション部起動
オニのプログラム部分
S7
システムデータ書換有?
N
S5
割込
アプリケーション部起動
オーのプログラム部分
S8
書換え指令チェック
S9
システムデータ書換え?
N
Y
S10
"システムデータを書き換えますか"
S11
書換え可?
Y
N
S12
書換え指令解除
S6
割込
アプリケーション部起動
オニのプログラム部分
S13
プログラムパターンチェック
S14
ウィルス有?
N
Y
書込み指令解除
S15
S16
"ウィルス注意"
S17
割込み解除